

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-175475

(43)公開日 平成11年(1999) 7月2日

(51)Int.Cl.⁸

識別記号

F I

G 0 6 F 15/00

3 3 0

G 0 6 F 15/00

3 3 0 B

13/00

3 5 1

13/00

3 5 1 Z

G 0 9 C 1/00

6 6 0

G 0 9 C 1/00

6 6 0 E

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 B

12/54

11/20

1 0 1 B

審査請求 未請求 請求項の数 3 O L (全 7 頁) 最終頁に続く

(21)出願番号

特願平9-341570

(22)出願日

平成9年(1997)12月11日

特許法第30条第1項適用申請有り 1997年11月6日～11月7日 社団法人情報処理学会開催の「第85回マルチメディア通信と分散処理研究会」において文書をもって発表

(71)出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72)発明者 清水 亮博

東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内

(72)発明者 山中 顯次郎

東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内

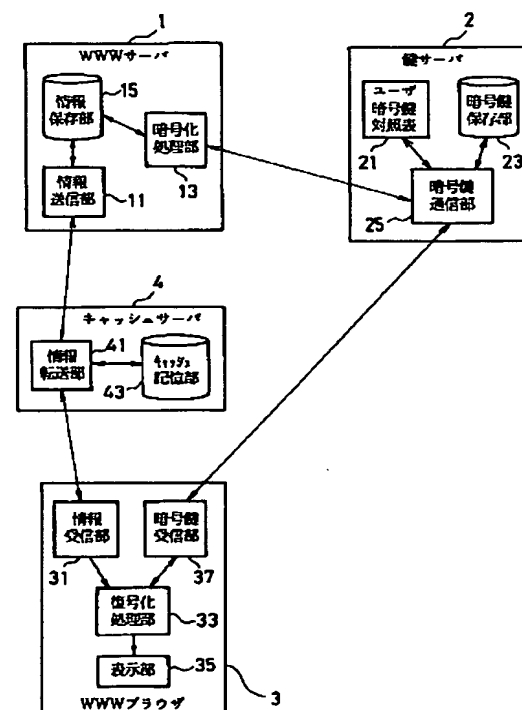
(74)代理人 弁理士 三好 秀和 (外1名)

(54)【発明の名称】 アクセス制御方法およびアクセス制御プログラムを記録した記録媒体

(57)【要約】

【課題】 ネットワークキャッシュによる情報提供者であるWWWサーバの負荷およびネットワーク自体の負荷を軽減しつつ条件を満たす利用者のみにコンテンツの閲覧を許容するアクセス制御方法およびアクセス制御プログラムを記録した記録媒体を提供する。

【解決手段】 WWWサーバ1にコンテンツを予め暗号化して記憶し、この暗号化コンテンツをWWWブラウザ3でメッセージとして受信し、該メッセージのトランスファーエンコーディングヘッダから鍵サーバのIPアドレスを調べ、暗号鍵IDとユーザ認証情報を鍵サーバ2に送信し、鍵サーバ2においてはWWWブラウザ3から受け取ったユーザ情報より暗号鍵IDに該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に暗号鍵をWWWブラウザ3に返送し、WWWブラウザ3は暗号鍵で暗号化コンテンツを復号する。



【特許請求の範囲】

【請求項 1】 インターネットにおける WWWサーバと WWWブラウザを有する情報提供システムにおいて、WWWサーバはコンテンツを予め暗号化して記憶し、WWWブラウザからの情報要求に対して前記暗号化されたコンテンツをメッセージとして WWWブラウザに配送し、所定の条件を満たす WWWブラウザにのみ暗号を解く暗号鍵を別途配送し、WWWブラウザは該暗号鍵で前記暗号化されたコンテンツを復号化することを特徴とするアクセス制御方法。

【請求項 2】 前記 WWWブラウザに暗号化鍵を別途配送する処理は、前記暗号化されたコンテンツを含むメッセージを受け取った WWWブラウザが該メッセージのトランスファーエンコーディング(Transfer-Encoding) ヘッダから鍵サーバの IP アドレスを調べ、暗号鍵 ID とユーザ認証情報を鍵サーバに送信し、鍵サーバは WWWブラウザから受け取ったユーザ情報より暗号鍵 ID に該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に前記暗号鍵を WWWブラウザに返送することを特徴とする請求項 1 記載のアクセス制御方法。

【請求項 3】 インターネットにおける WWWサーバと WWWブラウザを有する情報提供システムにおいて、WWWサーバにおいてはコンテンツを予め暗号化して記憶しておき、この暗号化されたコンテンツを WWWブラウザから WWWサーバに要求してメッセージとして WWWブラウザで受信し、WWWブラウザはこの受信したメッセージのトランスファーエンコーディング(Transfer-Encoding) ヘッダから鍵サーバの IP アドレスを調べ、暗号鍵 ID とユーザ認証情報を鍵サーバに送信し、鍵サーバにおいては WWWブラウザから受け取ったユーザ情報より暗号鍵 ID に該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に前記暗号鍵を WWWブラウザに返送し、WWWブラウザは該暗号鍵で前記暗号化されたコンテンツを復号化することを特徴とするアクセス制御プログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、インターネットにおいて WWW(World Wide Web) を使用して情報提供を行う際に有料コンテンツの保護またはセキュリティ保持のために利用者を制限すべく所定の条件を満たす利用者のみに情報の閲覧を許容するアクセス制御方法およびアクセス制御プログラムを記録した記録媒体に関する。

【0002】

【従来の技術】 インターネットの発展と、WWWの普及につれて、様々な情報がインターネット上で提供されるようになっていく。同時に情報のある特定の利用者へのみ見せたいとのニーズが高まっている。有料のコンテンツならば利用料を支払ったものだけに、秘密情報ならば

それを見る権限がある者だけに見せたい。ある条件を満たす者にのみ情報の閲覧を許す技術をアクセス制御と呼ぶ。

【0003】 従来のアクセス制御は、WWWサーバの情報転送機能と一体のものとして実現されていた。すなわち、条件を満たす利用者に予め ID とパスワードを発行し、WWWサーバへの情報要求の際に正しい ID とパスワードを入力しないと情報の転送自体を行わないとするものである。

10 【0004】

【発明が解決しようとする課題】 上述した従来のアクセス制御方法は、ネットワークキャッシュ技術との整合性が悪いという問題がある。

【0005】 ネットワークキャッシュ技術は、よく利用されるコンテンツをキャッシュサーバに保存しておき、そのコンテンツの要求に対しては WWWサーバの代わりにキャッシュサーバが情報の転送を行うものであり、WWWサーバとネットワークの負荷を軽減できるため、近年急速に普及している。

20 【0006】 しかしながら、キャッシュサーバは、情報要求が条件を満たす利用者からのものであるのかどうか判断できないため、従来型のアクセス制御が行われているコンテンツの代理転送を一切行わないので、ネットワークキャッシュによる WWWサーバおよびネットワークの負荷を軽減することができないというメリットを享受できないという問題がある。

30 【0007】 本発明は、上記に鑑みてなされたもので、その目的とするところは、ネットワークキャッシュによる情報提供者である WWWサーバの負荷およびネットワーク自体の負荷を軽減しつつ条件を満たす利用者のみにコンテンツの閲覧を許容するアクセス制御方法およびアクセス制御プログラムを記録した記録媒体を提供することにある。

【0008】

【課題を解決するための手段】 上記目的を達成するため、請求項 1 記載の本発明は、インターネットにおける WWWサーバと WWWブラウザを有する情報提供システムにおいて、WWWサーバはコンテンツを予め暗号化して記憶し、WWWブラウザからの情報要求に対して前記暗号化されたコンテンツをメッセージとして WWWブラウザに配送し、所定の条件を満たす WWWブラウザにのみ暗号を解く暗号鍵を別途配送し、WWWブラウザは該暗号鍵で前記暗号化されたコンテンツを復号化することを要旨とする。

50 【0009】 請求項 1 記載の本発明にあつては、WWWサーバはコンテンツを予め暗号化して記憶し、WWWブラウザからの要求に対して暗号化コンテンツを WWWブラウザに配送し、所定の条件を満たす WWWブラウザにのみ暗号を解く暗号鍵を別途配送し、WWWブラウザは該暗号鍵で暗号化コンテンツを復号化するため、ネット

3

ワークキャッシュ技術を有効に活用でき、WWWサーバの負荷およびネットワークの負荷を軽減することができる。すなわち、コンテンツを閲覧し得るか否かはWWWサーバでの情報の転送の許可、不許可でなく、WWWブラウザ側の利用者が暗号を解く鍵を持っているか否かであり、コンテンツは暗号化されているため、コンテンツの転送は無条件に許可され、誰にでも可能であり、キャッシュサーバにコンテンツを保持することができ、WWWサーバおよびネットワークの負荷を軽減することができる。

【0010】また、請求項2記載の本発明は、請求項1記載の発明において、前記WWWブラウザに暗号化鍵を別途配送する処理が、前記暗号化されたコンテンツを含むメッセージを受け取ったWWWブラウザが該メッセージのトランスファーエンコーディング(Transfer-Encoding)ヘッダから鍵サーバのIPアドレスを調べ、暗号鍵IDとユーザ認証情報を鍵サーバに送信し、鍵サーバはWWWブラウザから受け取ったユーザ情報より暗号鍵IDに該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に前記暗号鍵をWWWブラウザに返送することを要旨とする。

【0011】請求項2記載の本発明にあっては、暗号化コンテンツを含むメッセージを受け取ったWWWブラウザはメッセージのトランスファーエンコーディングヘッダから鍵サーバのIPアドレスを調べ、暗号鍵IDとユーザ認証情報を鍵サーバに送信し、鍵サーバはWWWブラウザからのユーザ情報より暗号鍵IDに該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に暗号鍵をWWWブラウザに返送するため、暗号化されたコンテンツを暗号鍵で復号化した場合のみコンテンツを閲覧でき、ネットワークキャッシュ技術を有効活用でき、WWWサーバの負荷およびネットワークの負荷を軽減することができる。なお、トランスファーエンコーディングヘッダはWWWサーバが用意するもので、そこに該当の暗号鍵のIDと登録されている鍵サーバのIPアドレスが記入されている。

【0012】更に、請求項3記載の本発明は、インターネットにおけるWWWサーバとWWWブラウザを有する情報提供システムにおいて、WWWサーバにおいてはコンテンツを予め暗号化して記憶しておき、この暗号化されたコンテンツをWWWブラウザからWWWサーバに要求してメッセージとしてWWWブラウザで受信し、WWWブラウザはこの受信したメッセージのトランスファーエンコーディング(Transfer-Encoding)ヘッダから鍵サーバのIPアドレスを調べ、暗号鍵IDとユーザ認証情報を鍵サーバに送信し、鍵サーバにおいてはWWWブラウザから受け取ったユーザ情報より暗号鍵IDに該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に前記暗号鍵をWWWブラウザに返送し、WWWブラウザは該暗号鍵で前記暗号化されたコンテン

4

ツを復号するアクセス制御プログラムを記録媒体に記録していることを要旨とする。

【0013】請求項3記載の本発明にあっては、WWWサーバにコンテンツを予め暗号化して記憶しておき、この暗号化コンテンツをWWWブラウザで受信し、トランスファーエンコーディングヘッダから鍵サーバのIPアドレスを調べ、暗号鍵IDとユーザ認証情報を鍵サーバに送信し、鍵サーバにおいてはWWWブラウザから受け取ったユーザ情報より暗号鍵IDに該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に暗号鍵をWWWブラウザに返送し、WWWブラウザは暗号鍵で暗号化コンテンツを復号するアクセス制御プログラムを記録媒体として記録しているため、該記録媒体を利用して、その流通性を高めることができる。

【0014】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【0015】図1は、本発明の一実施形態に係るアクセス制御方法を実施するシステム構成を示すブロック図である。図1において、1は情報の記憶および配送を行うWWWサーバ、2は暗号鍵の管理およびアクセス条件のチェックを行う鍵サーバ、3はWWWサーバ1に対して情報を要求し、WWWサーバ1から配送された情報を利用者に表示するWWWブラウザ、4はWWWサーバ1の情報を一時的に蓄積し、WWWサーバ1に代わって情報の配送を行うキャッシュサーバである。

【0016】WWWサーバ1は、情報送信部11、暗号化処理部13および情報保存部15から構成されている。情報送信部11は、WWWブラウザ3からの情報要求を受け取り、この要求された情報であるコンテンツを情報保存部15から取り出し、WWWブラウザ3に配送する。この時、コンテンツを暗号化して配送する場合には、配送メッセージのトランスファーエンコーディング(Transfer-Encoding)ヘッダによって暗号化されていることを示す。暗号化処理部13は、本アクセス制御方法のためのコンテンツの暗号化と鍵の鍵サーバ2への登録を行う。情報保存部15は、コンテンツおよび本アクセス制御方法の管理情報を記憶する。

【0017】鍵サーバ2は、ユーザ暗号鍵対照表21、暗号鍵保存部23および暗号鍵通信部25から構成されている。ユーザ暗号鍵対照表21は、利用者と該利用者がアクセス権を有する暗号鍵を対応して表形式に記憶する。暗号鍵保存部23は、WWWサーバ1から渡された暗号鍵を保存する。暗号鍵通信部25は、WWWサーバ1から暗号鍵およびアクセス情報を受け取って、ユーザ暗号鍵対照表21および暗号鍵保存部23に保存する。また、暗号鍵通信部25は、WWWブラウザ3から暗号鍵の要求を受け取り、この要求してきた利用者のアクセス権の有無をユーザ暗号鍵対照表21から調べ、アクセス権があれば暗号鍵をWWWブラウザ3に送る。

【0018】WWWブラウザ3は、情報受信部31、復号化処理部33、表示部35および暗号鍵受信部37から構成されている。情報受信部31は、WWWサーバ1に情報要求を送り、その応答を受信する。復号化処理部33は、情報受信部31を介してWWWサーバ1から受信した応答が暗号化されている場合に復号化を行う。表示部35は、復号化処理部33からの応答を表示する。暗号鍵受信部37は、鍵サーバ2に対して暗号鍵の要求を行い、鍵サーバ2から暗号鍵を受け取り、復号化処理部33に供給する。

【0019】キャッシュサーバ4は、情報転送部41およびキャッシュ記憶部43から構成されている。情報転送部41は、WWWブラウザ3からの情報要求をWWWサーバ1に中継し、WWWサーバ1からの応答をWWWブラウザ3に送るとともに、この応答をキャッシュ記憶部43に記憶しておく。なお、キャッシュサーバ4は通常のWWWで使用されるものと同一であり、本発明に固有な機能を特に必要としない。

【0020】次に、図2～図5を参照して、図1に示す実施形態の作用を説明する。

【0021】図2は、WWWサーバ1がWWWブラウザ3と通信する場合の通信制御処理を示すフローチャートである。図2において、WWWサーバ1は、WWWブラウザ3からの要求を受け付けると（ステップS11）、該要求を解釈して応答メッセージを用意する（ステップS13）。この時、WWWサーバ1は、WWWブラウザ3から要求された情報が暗号化されている場合には、

(1) 応答メッセージ本体が暗号化されていることを示す識別子、(2) 鍵サーバ2のIPアドレスを示す識別子、(3) 要求された情報を暗号化した暗号鍵の識別子を応答メッセージのトランスファーエンコーディング・ヘッダに添付して、WWWブラウザ3に返送する（ステップS17、S19）。

【0022】次に、図3に示すフローチャートを参照して、WWWブラウザ3がWWWサーバ1から応答メッセージを受け取って表示するまでの処理について説明する。

【0023】図3において、WWWブラウザ3は、WWWサーバ1から応答メッセージを受信すると（ステップS21）、メッセージのトランスファーエンコーディング・ヘッダに「メッセージ本体が暗号化されている」ことを示す識別子があるか否かをチェックする（ステップS23）。該識別子がある場合には、前記トランスファーエンコーディング・ヘッダから鍵サーバ2のIPアドレスと暗号鍵のIDを取得する（ステップS25）。それから、この取得したIPアドレスが示す鍵サーバ2と通信を行って、該鍵サーバ2からIDに該当する暗号鍵を受け取る（ステップS27）。そして、この暗号鍵を使用して、WWWサーバ1から受け取ったメッセージを復号化し（ステップS29）、この復号化したメッセー

ジを表示部35に表示する（ステップS31）。

【0024】次に、図4に示すフローチャートを参照して、鍵サーバ2とWWWブラウザ3との間における暗号鍵の受渡し処理について説明する。なお、図4において左側に示すフローチャートはWWWブラウザ3の暗号鍵受信処理を示し、右側のフローチャートは鍵サーバ2の鍵送信処理を示している。

【0025】図4において、鍵サーバ2がWWWブラウザ3からの接続を待っている状態において（ステップS51）、WWWブラウザ3が鍵サーバ2に接続されると（ステップS41）、鍵サーバ2はサーバ認証情報をWWWブラウザ3に送信する（ステップS52）。WWWブラウザ3は鍵サーバ2からサーバ認証情報を受信すると（ステップS42）、該サーバ認証情報を検査し、正しいサーバであることを確認する（ステップS43）。

【0026】WWWブラウザ3は、サーバ認証情報の確認後、ユーザ認証情報を鍵サーバ2に送信する（ステップS44）。鍵サーバ2は、WWWブラウザ3からのユーザ認証情報を受信すると（ステップS53）、この受信したユーザ認証情報を検査し、正しいユーザであるか否かを検査する（ステップS54）。WWWブラウザ3は、続いて暗号鍵の識別子を鍵サーバ2に送信する（ステップS45）。鍵サーバ2は、前記ユーザ認証情報から正しいユーザであることを確認し、更にWWWブラウザ3から暗号鍵の識別子を受信すると（ステップS55）、鍵サーバ2は、この受信した暗号鍵の識別子に該当する暗号鍵に対するアクセス権をユーザが持っているか否かをチェックする（ステップS56）。ユーザが該アクセス権を持っている場合には、鍵サーバ2は暗号鍵をWWWブラウザ3に返送し（ステップS57）、WWWブラウザ3は該暗号鍵を受信する（ステップS46）。

【0027】次に、図5に示すシーケンス図を参照して、図1に示す実施形態の全体的作用について説明する。図5において、まず情報がキャッシュされていない場合には、WWWブラウザ3からの情報要求はキャッシュサーバ4を経由してWWWサーバ1に送られ、WWWサーバ1は要求された情報を返信する。この返信情報はキャッシュサーバ4に一時的に保存されるとともにキャッシュサーバ4を経由してWWWブラウザ3に送信される。この情報が暗号化されている場合には、WWWブラウザ3は鍵サーバ2に対して暗号鍵を要求する。鍵サーバ2はこの要求に対して暗号鍵をWWWブラウザ3に返送し、WWWブラウザ3はこの暗号鍵を使用して、暗号化情報を復号する。

【0028】一方、情報がキャッシュされている場合には、WWWブラウザ3からの情報要求は、キャッシュサーバ4にて処理され、キャッシュサーバ4から情報がWWWブラウザ3に返信される。この情報が暗号化されている場合には、同様にWWWブラウザ3は鍵サーバ2に

対して暗号鍵を要求し、鍵サーバ2は暗号鍵をWWWブラウザ3に返送し、WWWブラウザ3はこの暗号鍵を使用して、暗号化情報を復号する。

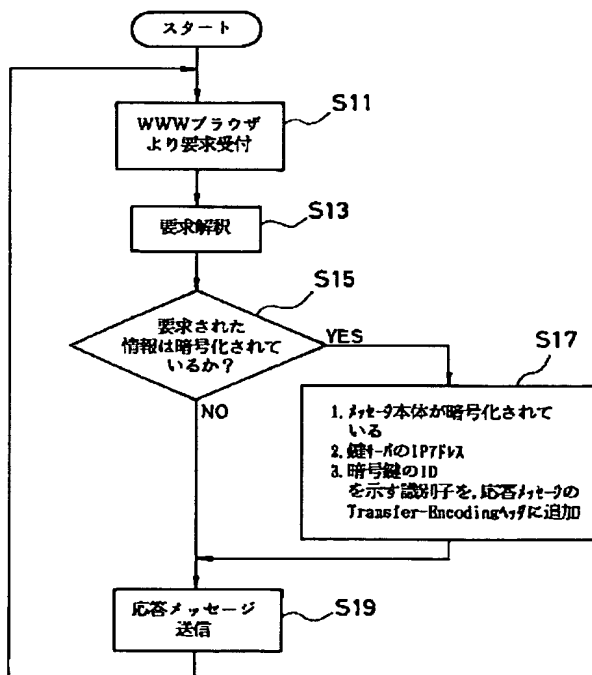
【0029】

【発明の効果】以上説明したように、本発明によれば、WWWサーバはコンテンツを予め暗号化して記憶し、WWWブラウザからの要求に対して暗号化コンテンツをWWWブラウザに配送し、所定の条件を満たすWWWブラウザにのみ暗号を解く暗号鍵を別途配送し、WWWブラウザは該暗号鍵で暗号化コンテンツを復号化するので、ネットワークキャッシュ技術を有効に活用でき、WWWサーバの能力が低くても大量の情報配信を行うことができ、多くの利用者に対する有料コンテンツの提供や秘密情報の提供を安価なハードウェアで実現できる。また、ネットワークへの負荷も軽減できるため、大量の情報の配信に伴うネットワークコストの上昇を抑制できる。更に、従来のアクセス制御では、通信の盗難によりコンテンツが漏洩する危険があったが、本発明ではコンテンツは暗号化されているため、このような危険を回避することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るアクセス制御方法を実施するシステム構成を示すブロック図である。

【図2】



【図2】図1の実施形態においてWWWサーバがWWWブラウザと通信する場合の通信制御処理を示すフローチャートである。

【図3】図1の実施形態においてWWWブラウザがWWWサーバから応答メッセージを受け取って表示するまでの処理を示すフローチャートである。

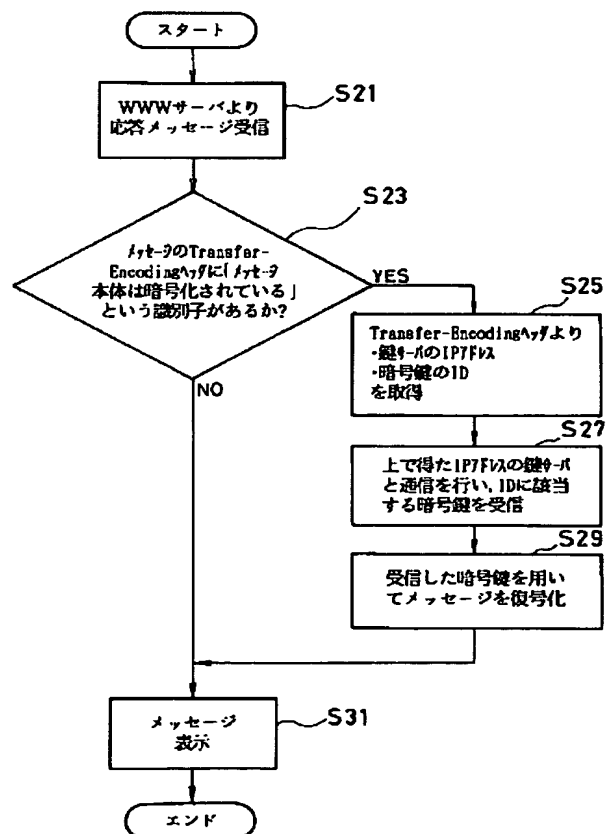
【図4】鍵サーバとWWWブラウザとの間における暗号鍵の受渡し処理を示すフローチャートである。

【図5】図1に示す実施形態の全体的作用を示すシーケンス図である。

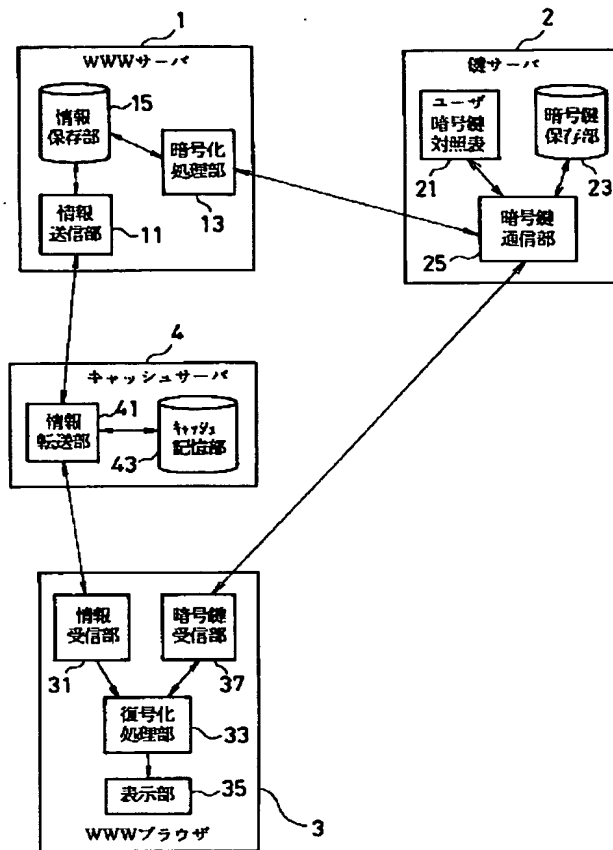
【符号の説明】

- 1 WWWサーバ
- 2 鍵サーバ
- 3 WWWブラウザ
- 4 キャッシュサーバ
- 13 暗号化処理部
- 15 情報保存部
- 21 ユーザ暗号鍵対照表
- 23 暗号鍵保存部
- 25 暗号鍵通信部
- 33 復号化処理部
- 37 暗号鍵受信部
- 43 キャッシュ記憶部

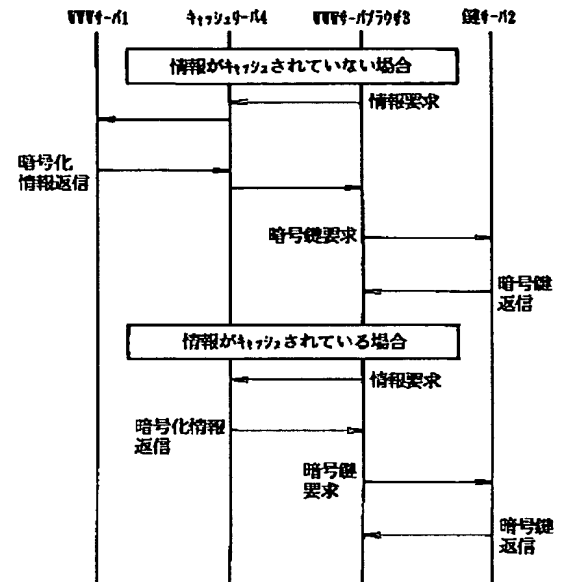
【図3】



【図 1】



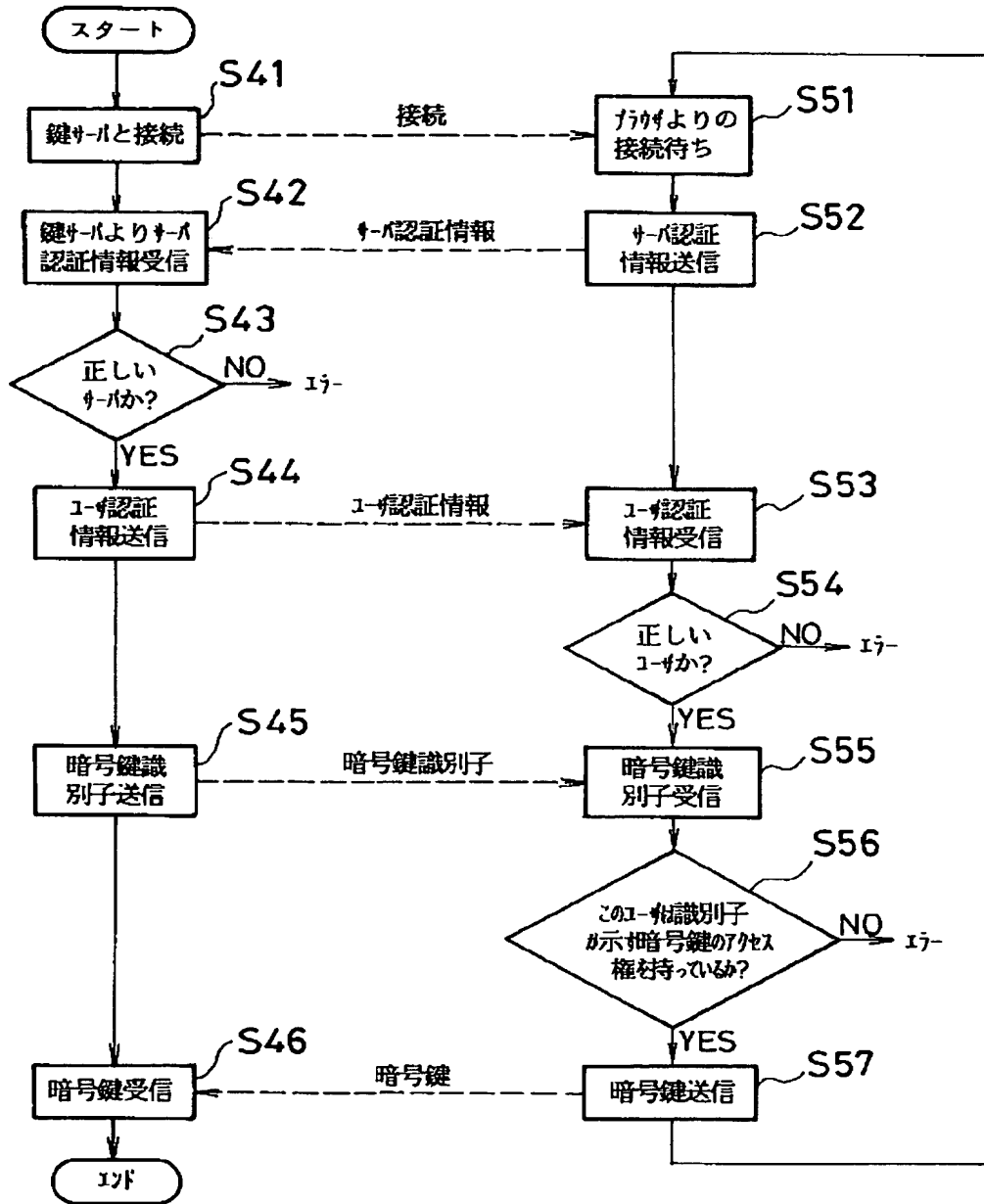
【図 5】



【図 4】

(サーバの暗号鍵受信機能)

(鍵サーバの鍵送信機能)



フロントページの続き

(51) Int. Cl. 6

識別記号

F I

H 0 4 L 12/58